

I claim:

1. A method of producing a stream of digital data comprising the step of:
determining a plurality of portions within the stream of digital data, such that
a portion of the stream of digital data is encrypted with an encryption key
that is capable of being decrypted by a decryption key and the portion including
therein another decryption key capable of decrypting a subsequent portion of the
stream of digital data, and
the subsequent portion of the stream of digital data is encrypted with
another encryption key that is capable of being decrypted by the another
decryption key; and
transmitting the stream of digital data, including the portion and the subsequent
portion.
2. A method according to claim 1 wherein the portion and a plurality of subsequent
portions comprise the plurality of portions, and each of the plurality of subsequent
portions is encrypted with a corresponding another encryption key, and within each of the
plurality of subsequent portions, except a last subsequent portion, there is included
therein a corresponding another decryption key capable of decrypting the corresponding
subsequent portion of the stream of digital data.
3. A method according to claim 2 wherein the encryption key and each another
encryption key is different and the decryption key and each another decryption key is
correspondingly different.

4. A method according to claim 3 wherein each encryption key, each another encryption key, each decryption key and each decryption key have a same key length.
5. A method according to claim 3 wherein the encryption key and decryption key certain ones of the another encryption keys and another decryption keys have a different key length.
6. A method according to claim 2 wherein the decryption key and each another decryption key is located at a different location within each portion.
7. A method according to claim 2 wherein each portion has a different bit size.
8. A method according to claim 2 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.
9. A method according to claim 8 wherein the encryption key and each another encryption key is different and the decryption key and each another decryption key is correspondingly different.
10. A method according to claim 9 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.

- [illegible]

17. A method according to claim 16 further including a marker that immediately precedes the decryption key and each another decryption key to allow identification of each another decryption key within the portion and subsequent portions, respectively.
18. A method according to claim 17 wherein each marker and the corresponding decryption key or another decryption key is encrypted in the same manner as the portion in which it is contained.
19. A method according to claim 1 further including a marker that immediately precedes the another decryption key to allow identification of the another decryption key within the portion.
20. A method according to claim 19 wherein the marker and the another decryption key is encrypted with the encryption key.
21. A method according to claim 20 wherein each encryption key is different and each decryption key is correspondingly different.
22. A method according to claim 21 wherein the corresponding decryption key in each different portion is not located at a same part of the portion.
23. A method according to claim 22 wherein each portion has a different size.

24. A method according to claim 22 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.

25. A method according to claim 19 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.

26. A method according to claim 1 further including, prior to the step of transmitting the stream of digital data, the steps of:

transmitting a decryption key that is capable of decrypting the portion of the stream of digital data; and

receiving an acknowledgement indicating that the decryption key has been properly installed on an end-user computer that will receive the transmitted stream of digital data.

27. A method according to claim 1 further including, prior to step of transmitting the stream of digital data, the steps of:

transmitting a set-up stream including an encrypted test decoder and an encrypted and encoded test sequence; and

receiving an acknowledgement with monitor information indicative of performance of an end-user computer; and

determining a key length and a key rotation period based upon the monitor information

28. A method according to claim 27 wherein the monitor information provides an amount of time required to decrypt and install the decryption key and decrypt and decode the test sequence.

29. A method according to claim 26 wherein, an encrypted executable decoder is included in the portion of the stream of digital data, the encrypted executable decoder, when decrypted and installed, being capable of decoding data content that is also included in the portion of the stream of digital data.

30. A method according to claim 29 wherein the encrypted executable decoder can be decrypted using the decryption key.

31. A method according to claim 26 wherein the portion and a plurality of subsequent portions comprise the plurality of portions, and each of the plurality of subsequent portions is encrypted with a corresponding another encryption key, and within each of the plurality of subsequent portions, except a last subsequent portion, there is including therein a corresponding another decryption key capable of decrypting the corresponding subsequent portion of the stream of digital data.

32. A method according to claim 31 wherein
the another decryption key is located within the portion at a location that precedes the end the portion by an amount that will ensure the remaining transmission time of the

portion after transmission of the another decryption key is greater than a latency measurement indicating an amount of time required to decrypt and install the decryption key; and

each another decryption key is located within each subsequent portion at another location that precedes the end the subsequent portion by another amount that will ensure the remaining transmission time of that subsequent portion after transmission of the corresponding another decryption key is greater than the latency measurement.

33. A method according to claim 31 wherein each encryption key is different and each decryption key is correspondingly different.

34. A method according to claim 33 wherein each encryption key, each another encryption key, each decryption key and each decryption key have a same key length.

35. A method according to claim 33 wherein the encryption key and decryption key and certain ones of the another encryption keys and another decryption keys have a different key length.

36. A method according to claim 31 wherein each portion has a different bit size.

37. A method according to claim 31 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.



38. A method according to claim 31 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.

39. A method according to claim 38 further including a marker that immediately precedes the decryption key and each another decryption key to allow identification of each another decryption key within the portion and subsequent portions, respectively.

40. A method according to claim 39 wherein the each marker and the corresponding decryption key or another decryption key is encrypted in the same manner as the portion in which it is contained.

41. A method according to claim 26 wherein the another decryption key is encrypted with the encryption key.

42. A method according to claim 26 further including a marker that immediately precedes the another decryption key to allow identification of the another decryption key within the portion.

43. A method according to claim 42 wherein the marker and the another decryption key is encrypted with the encryption key.

0982078-071604

44. A method according to claim 43 wherein the corresponding decryption key in each different portion is not located at a same part of the portion.
45. A method according to claim 44 wherein each portion has a different bit size.
46. A method according to claim 42 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.
47. A method according to claim 42 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.
48. A method according to claim 1 wherein:
- the portion immediately precedes the subsequent portion; and
 - the another decryption key is located within the portion at a location that precedes the end the portion by an amount that will ensure the remaining transmission time of the portion after transmission of the another decryption key is greater than a period of time needed to decrypt and install the another decryption key.
49. A method according to claim 48 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.

50. A transmission method comprising the steps of:

segmenting a stream of digital content into a plurality of portions;

inserting, into each of the plurality of portions except a last portion, one of a plurality of decryption keys that will be usable for decrypting a subsequent portion to obtain a modified stream;

encrypting each portion of the modified stream with an encryption key capable of being decrypted by a corresponding one of the plurality of decryption keys to obtain a plurality of encrypted portions;

attaching, onto each encrypted portion, a header identifying the one decryption key corresponding thereto to obtain a stream of digital data; and

transmitting the stream of digital data.

51. A method according to claim 50 wherein consecutive portions are encrypted with a different encryption key and capable of being decrypted with a different decryption key.

52. A method according to claim 51 wherein each of the portions contains a plurality of packets, and each of the packets contains the header identifying which decryption key to use to decrypt that packet.

53. A method according to claim 52 further including a marker that immediately precedes each of the plurality of decryption keys to allow identification of each of the plurality of decryption keys within each portion.

54. A method according to claim 50 wherein each of the portions contains a plurality of packets, and each of the packets contains the header identifying which decryption key to use to decrypt that packet.

55. A method according to claim 54 wherein each of the portions contains a plurality of packets, and each of the packets contains the header identifying which decryption key to use to decrypt that packet.

56. A method according to claim 55 further including a marker that immediately precedes each of the plurality of decryption keys to allow identification of each of the plurality of decryption keys within each portion.

57. A method according to claim 50 wherein each of the portions contains a plurality of packets, and each of the packets contains the header identifying which decryption key to use to decrypt that packet.

58. A method according to claim 57 further including a marker that immediately precedes each of the plurality of decryption keys to allow identification of each of the plurality of decryption keys within each portion.

59. A method according to claim 50 wherein each encryption key, each another encryption key, each decryption key and each decryption key have a same key length.

60. A method according to claim 50 wherein the encryption key and decryption key certain ones of the another encryption keys and another decryption keys have a different key length.
61. A method according to claim 50 wherein each of the plurality of decryption keys is located at a different location within each portion.
62. A method according to claim 50 wherein each portion has a different bit size.
63. A method according to claim 50 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.
64. A method according to claim 50 further including, prior to the step of transmitting the stream of digital data, the steps of:
- transmitting a decryption key that is capable of decrypting an initial portion of the stream of digital data; and
 - receiving an acknowledgement indicating that the decryption key has been properly installed on an end-user computer that will receive the transmitted stream of digital data.
65. A method according to claim 50 further including, prior to step of transmitting the stream of digital data, the steps of:

receiving an acknowledgement with monitor information indicative of performance of an end-user computer; and

66. A method according to claim 65 wherein the monitor information provides an amount of time required to decrypt and install the decryption key, and decrypt and decode the test sequence.

68. A method according to claim 50 wherein each of the subsequent decryption keys included in one of the portions is used to decrypt another portion that immediately follows the one portion.

32

receiving a portion of the stream digital data, the first portion being encrypted with an encryption key capable of being decrypted by a decryption key and including a subsequent decryption key capable of decrypting a subsequent portion of the stream of packets of digital data;

decrypting the portion of the stream of digital data using the decryption key;

identifying the subsequent decryption key disposed within the portion of the stream of digital data prior to completion of decrypting the portion of the stream of digital data;

installing the subsequent decryption key data prior to completion of decrypting the portion of the stream of digital data; and

receiving another portion of the stream of packets of digital data, the another portion being encrypted with another encryption key that is capable of being decrypted by the subsequent decryption key; and

decrypting the another portion of the stream of digital data using the subsequent decryption key.

70. A method according to claim 69 wherein the portion and the another portion each include a plurality of packets, and each of the packets contains a non-encrypted header identifying that the decryption key and the subsequent decryption key, respectively, should be used during the respective step of decrypting.

71. A method according to claim 70 wherein the step of identifying includes the step of locating a marker that immediately precedes the subsequent decryption key.

73. A method according to claim 71 further including additional steps of receiving and decrypting the another portion, and for each additional another portion, there is included

74. A method according to claim 73 wherein each memory address location for each additional subsequent decryption key is different.

34

76. A method according to claim 75 wherein each of the certain different decryption keys are located at a different location within the portion.

78. A method according to claim 77 wherein the step of receiving further includes the step of storing each certain different decryption key at a memory address location that is different from the from the immediately preceding certain different decryption key.

80. A method according to claim 79 wherein each portion includes a plurality of packets, and each of the packets contains a non-encrypted header identifying the decryption key that should be used during the step of decrypting.

35

82. A method according to claim 81 wherein each memory address location for each certain different decryption key is different.

83. An apparatus for producing a stream of digital data comprising:

means for determining a plurality of portions within the stream of digital data, such that

a portion of the stream of digital data is encrypted with an encryption key that is capable of being decrypted by a decryption key and the portion including therein another decryption key capable of decrypting a subsequent portion of the stream of digital data, and

the subsequent portion of the stream of digital data is encrypted with another encryption key that is capable of being decrypted by the another decryption key; and

means for transmitting the stream of digital data, including the portion and the subsequent portion.

84. An apparatus according to claim 83 wherein the portion and a plurality of subsequent portions comprise the plurality of portions, and each of the plurality of subsequent portions is encrypted with a corresponding another encryption key, and within each of the plurality of subsequent portions, except a last subsequent portion, there is included therein a corresponding another decryption key capable of decrypting the corresponding subsequent portion of the stream of digital data.

85. An apparatus according to claim 84 wherein the encryption key and each another encryption key is different and the decryption key and each another decryption key is correspondingly different.

86. An apparatus according to claim 85 wherein the encryption key and decryption key certain ones of the another encryption keys and another decryption keys have a different key length.

87. An apparatus according to claim 84 wherein the decryption key and each another decryption key is located at a different location within each portion.

88. An apparatus according to claim 84 wherein each portion has a different bit size.

89. An apparatus according to claim 84 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.

90. An apparatus according to claim 89 wherein the encryption key and each another encryption key is different and the decryption key and each another decryption key is correspondingly different.

91. An apparatus according to claim 89 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.

92. An apparatus according to claim 84 further including a marker that immediately precedes the decryption key and each another decryption key to allow identification of each another decryption key within the portion and subsequent portions, respectively.

93. An apparatus according to claim 92 wherein each marker and the corresponding decryption key or another decryption key is encrypted in the same manner as the portion in which it is contained.

94. An apparatus according to claim 83 wherein the another decryption key is encrypted with the encryption key.

95. An apparatus according to claim 94 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.

96. An apparatus according to claim 94 wherein the encryption key and each another encryption key is different and the decryption key and each another decryption key is correspondingly different.

97. An apparatus according to claim 95 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.

98. An apparatus according to claim 97 further including a marker that immediately precedes the decryption key and each another decryption key to allow identification of each another decryption key within the portion and subsequent portions, respectively.

99. An apparatus according to claim 98 wherein each marker and the corresponding decryption key or another decryption key is encrypted in the same manner as the portion in which it is contained.

100. An apparatus according to claim 83 further including a marker that immediately precedes the another decryption key to allow identification of the another decryption key within the portion.

101. An apparatus according to claim 100 wherein the marker and the another decryption key is encrypted with the encryption key.

102. An apparatus according to claim 101 wherein each encryption key is different and each decryption key is correspondingly different.

103. An apparatus according to claim 102 wherein the corresponding decryption key in each different portion is not located at a same part of the portion.

104. An apparatus according to claim 103 wherein each portion has a different size.

105. An apparatus according to claim 103 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.

106. An apparatus according to claim 100 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.

107. An apparatus according to claim 83 further including:

means for transmitting a decryption key that is capable of decrypting the portion of the stream of digital data; and

means for receiving an acknowledgement indicating that the decryption key has been properly installed on an end-user computer that will receive the transmitted stream of digital data.

108. An apparatus according to claim 83 further including:

means for transmitting a set-up stream including an encrypted test decoder and an encrypted and encoded test sequence; and

means for receiving an acknowledgement with monitor information indicative of performance of an end-user computer; and

means for determining a key length and a key rotation period based upon the monitor information.

109. An apparatus according to claim 108 wherein the monitor information provides an amount of time required to decrypt and install the decryption key and decrypt and decode the test sequence.

110. An apparatus according to claim 107 wherein, an encrypted executable decoder is included in the portion of the stream of digital data, the encrypted executable decoder, when decrypted and installed, being capable of decoding data content that is also included in the portion of the stream of digital data.

111. An apparatus according to claim 110 wherein the encrypted executable decoder can be decrypted using the decryption key.

112. An apparatus according to claim 107 wherein the portion and a plurality of subsequent portions comprise the plurality of portions, and each of the plurality of subsequent portions is encrypted with a corresponding another encryption key, and within each of the plurality of subsequent portions, except a last subsequent portion, there is including therein a corresponding another decryption key capable of decrypting the corresponding subsequent portion of the stream of digital data.

113. An apparatus according to claim 112 wherein

the another decryption key is located within the portion at a location that precedes the end the portion by an amount that will ensure the remaining transmission time of the portion after transmission of the another decryption key is greater than a latency measurement indicating an amount of time required to decrypt and install the decryption key; and

each another decryption key is located within each subsequent portion at another location that precedes the end the subsequent portion by another amount that will ensure the remaining transmission time of that subsequent portion after transmission of the corresponding another decryption key is greater than the latency measurement.

114. An apparatus according to claim 112 wherein each encryption key is different and each decryption key is correspondingly different.

115. An apparatus according to claim 114 wherein each encryption key, each another encryption key, each decryption key and each decryption key have a same key length.

116. An apparatus according to claim 114 wherein the encryption key and decryption key and certain ones of the another encryption keys and another decryption keys have a different key length.

117. An apparatus according to claim 114 wherein each portion has a different bit size.

118. An apparatus according to claim 114 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.

119. An apparatus according to claim 114 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.

120. An apparatus according to claim 119 further including a marker that immediately precedes the decryption key and each another decryption key to allow identification of each another decryption key within the portion and subsequent portions, respectively.

121. An apparatus according to claim 120 wherein the each marker and the corresponding decryption key or another decryption key is encrypted in the same manner as the portion in which it is contained.

122. An apparatus according to claim 107 wherein the another decryption key is encrypted with the encryption key.

123. An apparatus according to claim 107 further including a marker that immediately precedes the another decryption key to allow identification of the another decryption key within the portion.

124. An apparatus according to claim 123 wherein the marker and the another decryption key is encrypted with the encryption key.
125. An apparatus according to claim 124 wherein the corresponding decryption key in each different portion is not located at a same part of the portion.
126. An apparatus according to claim 125 wherein each portion has a different bit size.
127. An apparatus according to claim 123 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.
128. An apparatus according to claim 123 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.
129. An apparatus according to claim 83 wherein:
- the portion immediately precedes the subsequent portion; and
 - the another decryption key is located within the portion at a location that precedes the end the portion by an amount that will ensure the remaining transmission time of the portion after transmission of the another decryption key is greater than a period of time needed to decrypt and install the another decryption key.

130. An apparatus according to claim 129 wherein each of the portions contains a plurality of packets, and each of the packets contains a non-encrypted header identifying which decryption key to use to decrypt that packet.

131. A transmission apparatus comprising:

means for segmenting a stream of digital content into a plurality of portions;

means for inserting, into each of the plurality of portions except a last portion, one of a plurality of decryption keys that will be usable for decrypting a subsequent portion to obtain a modified stream;

means for encrypting each portion of the modified stream with an encryption key capable of being decrypted by a corresponding one of the plurality of decryption keys to obtain a plurality of encrypted portions;

means for attaching, onto each encrypted portion, a header identifying the one decryption key corresponding thereto to obtain a stream of digital data; and

means for transmitting the stream of digital data.

132. An apparatus according to claim 131 wherein consecutive portions are encrypted with a different encryption key and capable of being decrypted with a different decryption key.

133. An apparatus according to claim 132 wherein each of the portions contains a plurality of packets, and each of the packets contains the header identifying which decryption key to use to decrypt that packet.

134. An apparatus according to claim 133 further including a marker that immediately precedes each of the plurality of decryption keys to allow identification of each of the plurality of decryption keys within each portion.

135. An apparatus according to claim 131 wherein each of the portions contains a plurality of packets, and each of the packets contains the header identifying which decryption key to use to decrypt that packet.

136. An apparatus according to claim 135 wherein each of the portions contains a plurality of packets, and each of the packets contains the header identifying which decryption key to use to decrypt that packet.

137. An apparatus according to claim 136 further including a marker that immediately precedes each of the plurality of decryption keys to allow identification of each of the plurality of decryption keys within each portion.

138. An apparatus according to claim 131 wherein each of the portions contains a plurality of packets, and each of the packets contains the header identifying which decryption key to use to decrypt that packet.

139. An apparatus according to claim 138 further including a marker that immediately precedes each of the plurality of decryption keys to allow identification of each of the plurality of decryption keys within each portion.

140. An apparatus according to claim 131 wherein each encryption key, each another encryption key, each decryption key and each decryption key have a same key length.

141. An apparatus according to claim 131 wherein the encryption key and decryption key certain ones of the another encryption keys and another decryption keys have a different key length.

142. An apparatus according to claim 131 wherein each of the plurality of decryption keys is located at a different location within each portion.

143. An apparatus according to claim 131 wherein each portion has a different bit size.

144. An apparatus according to claim 131 wherein the plurality of portions are transmitted in an order corresponding to a playback sequence.

145. An apparatus according to claim 131 further:

means for transmitting a decryption key that is capable of decrypting an initial portion of the stream of digital data; and

means for receiving an acknowledgement indicating that the decryption key has been properly installed on an end-user computer that will receive the transmitted stream of digital data.

146. An apparatus according to claim 131 further:

means for transmitting a set-up stream including an encrypted test decoder and an encrypted and encoded test sequence; and

means for receiving an acknowledgement with monitor information indicative of performance of an end-user computer; and

means for determining a key length and a key rotation period based upon the monitor information.

147. An apparatus according to claim 146 wherein the monitor information provides an amount of time required to decrypt and install the decryption key, and decrypt and decode the test sequence.

148. An apparatus according to claim 131 wherein, an encrypted executable decoder is included in an initial portion of the stream of digital data, the encrypted executable decoder, when decrypted and installed, being capable of decoding data content that is also included in the portion of the stream of digital data.

149. An apparatus according to claim 131 wherein each of the subsequent decryption keys included in one of the portions is used to decrypt another portion that immediately follows the one portion.

150. An apparatus for decrypting a stream of digital data comprising:

means for receiving a portion of the stream digital data, the first portion being encrypted with an encryption key capable of being decrypted by a decryption key and including a subsequent decryption key capable of decrypting a subsequent portion of the stream of packets of digital data;

means for decrypting the portion of the stream of digital data using the decryption key;

means for identifying the subsequent decryption key disposed within the portion of the stream of digital data prior to completion of decrypting the portion of the stream of digital data;

means for installing the subsequent decryption key data prior to completion of decrypting the portion of the stream of digital data; and

means for receiving another portion of the stream of packets of digital data, the another portion being encrypted with another encryption key that is capable of being decrypted by the subsequent decryption key; and

means for decrypting the another portion of the stream of digital data using the subsequent decryption key.

151. An apparatus according to claim 150 wherein the portion and the another portion each include a plurality of packets, and each of the packets contains a non-encrypted header identifying that the decryption key and the subsequent decryption key, respectively, should be used during the respective step of decrypting.

152. An apparatus according to claim 151 wherein the step of identifying includes the step of locating a marker that immediately precedes the subsequent decryption key.

153. An apparatus according to claim 152 wherein the step of installing stores the subsequent decryption key at a memory address location that is different from the decryption key.

154. An apparatus according to claim 152 further the means for receiving and decrypting are capable of receiving and decrypting additional another portions, and the means for installing stores each additional subsequent decryption key at a memory address location that is different from the immediately preceding subsequent decryption key.

155. An apparatus according to claim 154 wherein each memory address location for each additional subsequent decryption key is different.